



Données personnelles : Facebook ne peut pas enregistrer les données de navigation des internautes sans leur consentement

Boris Barraud

► To cite this version:

Boris Barraud. Données personnelles : Facebook ne peut pas enregistrer les données de navigation des internautes sans leur consentement. *Revue européenne des médias et du numérique*, 2016, 37, p. 23 s. hal-01367682

HAL Id: hal-01367682

<https://hal-amu.archives-ouvertes.fr/hal-01367682>

Submitted on 16 Sep 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Boris Barraud, « Données personnelles : Facebook ne peut pas enregistrer les données de navigation des internautes sans leur consentement », *Revue Européenne des Médias et du Numérique* 2016, n° 37, p. 23 s.

manuscrit de l'auteur



Les données personnelles sont le pétrole du XXI^e s. Et Facebook est, si ce n'est le roi du pétrole, au moins un roi du pétrole, capable de revendre à prix d'or les informations privées relatives à ses utilisateurs à d'innombrables annonceurs. Évidemment, ce modèle économique interroge diverses législations et notamment celle relative à la préservation de la vie privée. En novembre 2014, l'incontournable réseau social annonçait une grande révision de ses conditions d'utilisation et, en particulier, de sa « Déclaration des droits et responsabilités ». Entrés en vigueur le 30 janvier 2015, ces changements n'ont pas manqué d'attirer l'attention des autorités publiques en charge de la protection des données personnelles.

Peut-être est-ce la Commission de la protection de la vie privée belge (CPVP, équivalent de la CNIL française) qui a dès lors le plus strictement surveillé les activités et les procédés de l'entreprise californienne. En tout cas, cette commission a engagé un bras de fer autour du cookie « Datr » et de la pratique consistant à pister tous les internautes, y compris ceux qui sont déconnectés du service et même ceux qui ne sont pas inscrits, qui ne possèdent pas de comptes personnels. Facebook ne se conformant pas aux recommandations de l'autorité belge, celle-ci l'a attaqué en justice, laquelle a lourdement sanctionné la société américaine. Pendant ce temps, l'annonce de la révision des conditions d'utilisation de Facebook a amené les instances en charge de la sauvegarde des données personnelles de cinq pays européens (Pays-Bas, France, Espagne, Allemagne et Belgique) à se réunir et à créer un Groupe de contact afin d'harmoniser leurs réponses face aux nouvelles menaces que ferait peser Facebook. Or ce Groupe de contact a récemment fait sienne la décision de justice belge, contribuant à toujours plus resserrer l'étau autour du réseau social, qui peut de moins en moins librement pêcher les informations privées au moyen de ses célèbres hameçons : le bouton « J'aime » et le bouton « Partager ».

La technologie incriminée : le cookie « Datr »

Grâce à ses outils de partage et de recommandation présents sur de plus en plus de pages web, Facebook est en mesure d'enregistrer nombre d'informations relatives aux sites consultés par les internautes. Et, lorsque ceux-ci ne sont pas identifiés avec un compte Facebook, les données sont rattachées à des numéros d'identifiant uniques, lesquels permettent d'établir des profils précis afin d'afficher des publicités ciblées. C'est le cookie « Datr » qui permet cela, un cookie étant un micro-fichier installé dans le navigateur d'un internaute et capable de mémoriser différents types d'informations le concernant. Facebook dépose systématiquement ce cookie sur le terminal (ordinateur, tablette, mobile) de tout internaute qui consulte une page quelconque du domaine <facebook.com> — par exemple la page publique d'un événement ou d'une personnalité —, y compris lorsque l'utilisateur n'a jamais ouvert de compte et est donc un « utilisateur passif » du réseau social. Dès lors, à chaque fois que l'internaute ouvre une page web contenant un plug-in Facebook, la société américaine enregistre l'information selon laquelle il s'est rendu sur cette page, y compris, donc, si l'utilisateur n'est pas identifié avec un compte Facebook.

Le bouton « J'aime » est, selon Quantcast Ranking, implémenté sur 32 % des 10 000 sites web les plus visités. Seulement l'internaute qui entend informer la communauté Facebook ou ses amis Facebook qu'il aime tel ou tel produit ou tel ou tel chanteur comprend-il, normalement, qu'il en informe également l'entreprise qui lui délivre le service de réseautage social. Le cookie « Datr », lui, est un moyen déguisé et insidieux d'observer les activités des internautes puisqu'il est utilisé à l'égard de personnes non membres du réseau social et loin de tous actes positifs tels que le fait de cliquer sur le bouton « J'aime ». En outre, ce cookie est conservé sur le disque dur de tout visiteur de <facebook.com> pendant deux années, si bien qu'il est possible d'être surveillé par Facebook tout en ne s'étant pas rendu sur le site web du réseau social depuis des mois.

Un rapport soulignant les graves atteintes à la vie privée commises par Facebook

Après l'annonce de la modification de ses conditions d'utilisation, Facebook a fait l'objet d'une enquête approfondie menée par des chercheurs de la Katholieke Universiteit de Louvain et de la Vrije Universiteit de Bruxelles et commandée par la CPVP. Les conclusions desdits chercheurs, rendues publiques en février 2015, ont mis en exergue les risques que feraient planer sur la préservation de la vie privée le contrat d'utilisation du service. Surtout, elles ont relevé le caractère systématique et massif de la collecte de données personnelles d'internautes non membres par Facebook grâce au cookie « Datr ». Et de reprocher à Facebook d'enfreindre en conséquence de multiples lois sur la protection des données personnelles ainsi que la réglementation européenne en la matière.

Au final, il est apparu que Facebook collecte des informations personnelles sans le consentement éclairé de ses utilisateurs et sans aucun consentement de ses non-utilisateurs, avec lesquels aucun contrat n'a été signé et qui pour la plupart ne peuvent se douter qu'ils sont ainsi pistés dans nombre de leurs activités en ligne. Si la variété des données collectées est moins importante concernant les internautes non-membres et concernant les internautes membres déconnectés que concernant les internautes membres connectés — les chercheurs ont noté que Facebook enregistre dans ce cas 11 types d'informations —, l'atteinte à l'intimité n'en est pas moins patente. Ce sont jusqu'aux données sensibles telles que des renseignements médicaux ou les préférences religieuses, sexuelles ou politiques qui peuvent être recensées.

Facebook poursuivi par la Commission de la protection de la vie privée belge

Aussi la CPVP a-t-elle fermement réagi suite à ce rapport. Tout d'abord, en mai 2015, elle a menacé Facebook de poursuites judiciaires et a exigé de lui qu'il

cesse immédiatement de pister au moins les internautes non inscrits, donc qu'il n'utilise plus le fameux cookie « Datr ». Elle a également demandé le retrait des outils qui permettent d'identifier et de suivre les internautes en dehors du réseau social, comme « Facebook Connect ». Selon la CPVP, un service de réseautage social en ligne ne peut collecter des informations personnelles par le biais de cookies et de modules sociaux qu'après avoir obtenu le « consentement indubitable et spécifique des personnes concernées, via un opt-in et dans la mesure où cela est strictement nécessaire au fonctionnement du service ». Le mécanisme d'opt-out « ne convient pas pour obtenir un consentement informé de l'utilisateur moyen », au sens du régulateur belge. Les services tels que Facebook, qui se rémunèrent par le vente de leurs utilisateurs à des annonceurs, jouent logiquement sur le manque de transparence de leurs conditions d'utilisation, si bien que celles-ci ne sont que très rarement comprises par ceux qui s'inscrivent et qui donc « acceptent » supposément ces conditions.

Ensuite, devant le refus de coopérer de la société californienne, la « CNIL belge » l'a assignée en justice, en juin 2015, dénonçant un traçage « invasif » par Facebook des habitudes de navigation des internautes forcément incompatible avec le droit des données personnelles et, en premier lieu, avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Ce n'est toutefois que le problème du suivi des activités en ligne des personnes non inscrites au réseau social qui a focalisé toute l'attention et qui a conduit à la lourde condamnation de Facebook par la justice belge. Les juges ont donc donné raison à la CPVP selon laquelle il n'est pas légal de « collecter systématiquement des données relatives à la consultation de sites internet externes mais qui contiennent des modules sociaux [...], alors même que l'internaute n'interagit pas avec ces modules sociaux ».

Facebook lourdement condamné par la justice belge

Le 9 novembre 2015, à travers une ordonnance longue de 33 pages, le tribunal de première instance néerlandophone de Bruxelles — après avoir tout d'abord réaffirmé la compétence de la juridiction belge, en constatant que les activités du responsable de traitement (Facebook Inc.) et celles de la SPRL Facebook Belgium sont indissociablement liées — a suivi les griefs de la CPVP et a imposé à Facebook Inc., Facebook Belgium SPRL et Facebook Ireland Limited de cesser de déposer le cookie « Datr » lorsque des internautes non inscrits visitent le site <facebook.com> sans les en informer au préalable et de manière claire. Facebook devra à l'avenir demander expressément l'accord des internautes belges non membres du réseau social et leur fournir des explications suffisantes quant à l'usage fait des données recueillies. Or il est évidemment difficile pour un service d'obtenir quelque autorisation expresse de la part de personnes qui ne sont pas inscrites à ce service. Les juges ont donc requis de Facebook qu'il arrête de collecter des informations personnelles relativement à ses « utilisateurs passifs » par l'intermédiaire de plug-ins

placés sur des sites web tiers. Facebook devait mettre fin à cette pratique dans les 48 heures suivant la signification de l'ordonnance sous peine d'une astreinte élevée de 250 000 euros par jour de retard. La société américaine a fait appel, mais celui-ci n'est pas suspensif.

Cette décision de la justice belge est inédite et d'une grande importance en ce que c'est une part du modèle économique du méga-réseau social qui pourrait être impactée, surtout si les justices d'autres pays en venaient à suivre l'impulsion donnée par le tribunal de Bruxelles. Il est défendu à Facebook de tracer les internautes sans leur consentement et cela risque d'impacter le fonctionnement du service, pour l'instant à l'échelle de la Belgique et bientôt peut-être à une échelle autrement significative. Il faut toutefois souligner que cette ordonnance ne concerne que les internautes qui n'ont ouvert aucun compte auprès de Facebook et que, en l'état, ceux qui ont ouvert un tel compte sont réputés avoir consenti expressément à ce que l'entreprise californienne exploite commercialement leurs données. Or ce sont surtout ces derniers, les « utilisateurs actifs », qui présentent une valeur marchande aux yeux de ladite entreprise.

La vigilance des autorités de protection des données personnelles européennes

Reste que, pour Facebook, le couperet se rapproche, cette décision de justice risquant de faire tâche d'huile dans toute l'Europe. Nul doute que, au regard d'autres droits nationaux et, surtout, au regard du droit européen, les ingérences dans la vie privée d'internautes qui n'ont réellement fait aucun geste positif en ce sens ne sont guère admissibles. Et ce qui vaut pour Facebook vaut également à l'égard d'autres sociétés dont l'activité consiste — suivant une expression peut-être encore plus valide à l'égard du web qu'à l'égard de la télévision — à « vendre du temps de cerveau disponible à des annonceurs », au premier rang desquelles figure Google.

En ce sens, les autorités de protection des données personnelles membres du Groupe de contact précédemment évoqué ont, le 4 décembre 2015, publié une déclaration commune afin de prendre acte de l'ordonnance du tribunal de Bruxelles et afin de demander à Facebook de « se conforme[r] au jugement sur tout le territoire de l'Union Européenne, et [de] pren[dre] toute mesure pour se mettre en conformité avec la législation européenne », soit avec les obligations issues des directives 95/46/EC du 24 octobre 1995, *Relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, et 2002/58/EC du 12 juillet 2002, *Concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*. Cette déclaration commune ne constitue peut-être que les prémices d'une réaction de plus grande envergure, face aux atteintes aux données personnelles dont se rendent coupables certains services, de la part de chaque « CNIL nationale » et de la part du G29 (groupe des « CNIL européennes »).

La défense et la réaction du réseau social

Facebook se défend en arguant que le cookie « Datr » servirait essentiellement à protéger les utilisateurs en identifiant leurs navigateurs pour minimiser les risques de piratage et de création de faux comptes. En octobre 2015, le responsable de la sécurité de Facebook, Alex Stamos, avait ainsi expliqué dans un billet publié sur le réseau social que ce cookie permettrait de « différencier les visites légitimes des visites illégitimes », donc de distinguer les internautes des robots malveillants qui parcourent la toile. Et l'entreprise de préciser, dans un communiqué faisant suite à la décision de justice belge, qu'elle utilisait le cookie incriminé « depuis plus de cinq ans afin que Facebook reste sécurisé pour 1,5 milliard de personnes à travers le monde ».

Par ailleurs, Facebook s'est bel et bien conformé à l'ordonnance du tribunal de Bruxelles, mais d'une façon assez inattendue : plutôt que de neutraliser le cookie litigieux, le réseau social a préféré interdire l'accès à <facebook.com> aux internautes belges non connectés au service. Il n'est donc plus possible, sur le territoire belge, de consulter librement, sans posséder un compte et sans être connecté, les contenus publics qui sont mis en ligne. Cela a entraîné une nouvelle réaction de la CPVP, son président, Willem Debeuckelaere, fustigeant l'attitude de Facebook et résumant : « Ce n'est pas ce que nous avons demandé ». Facebook entend bien procéder à du chantage en faisant passer les autorités publiques pour de dangereux Léviathans liberticides ; et il en a les moyens. Reste aux dites autorités publiques à faire preuve de pédagogie et à enseigner aux internautes comme aux dirigeants de Facebook qu'il n'est pas de liberté sans vie privée.